1964

Subdirect sums of rings

R. J. McNells
Lehigh University

ABSTRACT

The notion of subdirect sum of a set of rings is a generalization of the familiar concept of direct sum and enables one to prove representation theorems concerning general rings; i.e. rings not necessarily satisfying finiteness assumptions. It is the purpose of this thesis to organize some of the fundamental theorems of subdirect sums of rings.

We begin by defining the notion of subdirect sum and some related concepts after which we state and prove two theorems which are fundamental in the theory. These theorems give necessary and sufficient conditions for an arbitrary ring to have a representation as a subdirect sum of a set of rings.

The second chapter develops the notion of subdirectly irreducible rings and gives the important theorem that any ring is isomorphic to a subdirect sum of subdirectly irreducible rings. We also show that this representation, and hence subdirect sum representations, need not be unique,

In particular instances the first of two questions posed in the Introduction is answered in Chapter III. Under which conditions does a given ring have a representation as a subdirect sum of some specified class of rings? The question is answered (Theorem 10) when the given class of rings is a class of fields I/(p), p a prime, and when the class of rings is a class of division rings (Theorem 11).

The final section is concerned with prime rings and their subdirect sum representations. Several lemmas regarding

countable prime rings are proved and these form the background material for the principal theorem of the section. This theorem illustrates the second problem stated in the Introduction. We are given a countable set of prime rings R_i and a ring R of some specific type. We wish to determine under which conditions $R[x]$ has a representation as a subdirect sum of the R_i.

SUBDIRECT SUMS OF RINGS

by

Robert Joseph McNelis

A THESIS

Presented to the Graduate Faculty

of Lehigh University

in Candidacy for the Degree of

Master of Science

Lehigh University

1964

CERTIFICATE OF APPROVAL

This thesis is accepted and approved in partial fulfillment of the requirements for the degree of Master of Science.

May 20, 1964
(date)

Harry Larson
Professor in charge

Ernest Pickett
Head of the Department

CERTIFICATE OF APPROVAL

This thesis is accepted and approved in partial fulfillment of the requirements for the degree of Master of Science.

May 20, 1964
(date)

Harry Larson
Professor in charge

Ernest Pickett
Head of the Department

ACKNOWLEDGEMENTS

I wish to express my sincere thanks to Mr. Gary B. Laison for his help in directing this thesis and to Dr. Mario Petrich for his helpful suggestions.

TABLE OF CONTENTS

ABSTRACT

The notion of subdirect sum of a set of rings is a generalization of the familiar concept of direct sum and enables one to prove representation theorems concerning general rings; i.e. rings not necessarily satisfying finiteness assumptions. It is the purpose of this thesis to organize some of the fundamental theorems of subdirect sums of rings.

We begin by defining the notion of subdirect sum and some related concepts after which we state and prove two theorems which are fundamental in the theory. These theorems give necessary and sufficient conditions for an arbitrary ring to have a representation as a subdirect sum of a set of rings.

The second chapter develops the notion of subdirectly irreducible rings and gives the important theorem that any ring is isomorphic to a subdirect sum of subdirectly irreducible rings. We also show that this representation, and hence subdirect sum representations, need not be unique.

In particular instances the first of two questions posed in the Introduction is answered in Chapter III. Under which conditions does a given ring have a representation as a subdirect sum of some specified class of rings? The question is answered (Theorem 10) when the given class of rings is a class fields $I/(p)$, p a prime, and when the class of rings is a class of division rings (Theorem 11).

The final section is concerned with prime rings and their subdirect sum representations. Several lemmas regarding

countable prime rings are proved and these form the background material for the principal theorem of the section. This theorem illustrates the second problem stated in the Introduction. We are given a countable set of prime rings R_i and a ring R of some specific type. We wish to determine under which conditions R[x] has a representation as a subdirect sum of the R_i.

INTRODUCTION

The concept of direct sum is fundamental in the study of any algebraic system including the theory of rings. In this theory the rings under consideration are usually assumed to satisfy certain finiteness assumptions (e.g. the descending chain condition) and this is conducive to theorems concerning direct sums. In the case of general rings, however, many of these theorems become invalid indicating that the direct sum concept is somewhat inadequate. It has been found that an arbitrary ring R may be isomorphic to a subring of a direct sum of certain rings S_i, but not to a complete direct sum of these rings. With this in mind the notion of subdirect sum is defined to include that of direct sum, but in doing so some of the basic properties of the latter are lost. For example, the direct sum of a given set of rings S_i is unique up to isomorphism while there may exist many different subdirect sums of the S_i. (An example is given at the end of the second chapter.)

It is natural, then, to investigate the conditions under which a given ring has a unique subdirect sum representation. In my reading I have not encountered any theorem which states necessary and sufficient conditions for such uniqueness.

Several questions have been answered however by early contributors to the theory. Given a ring R, does it have representations as a subdirect sum? What are the necessary

and sufficient conditions for a given ring R to have a representation as a subdirect sum of a specified class of rings? Conversely, given a set of rings $\{S_i\}$ does there exist among the various subdirect sums of these rings one which is isomorphic to a ring S of some specific type? The first three questions have been fully investigated by H. Prufer (1925), W. Krull (1929), G. Kothe (1930), M.H. Stone (1936) and later by N.H. McCoy. The converse problem, on the other hand, is a more difficult one not being studied in as great detail. In this area Krull came forward with the first major results which were later expanded by McCoy.

The study of subdirect sums is extensive and I do not pretend to exhaust the field. For example, the relation between radicals and subdirectsums is not discussed. Nevertheless, I attempt to state and prove important theorems thus far developed which are fundamental in the theory. All the questions in the preceding paragraph are treated at length.

The numbers in the brackets following an author's name refer to the bibliography.

CHAPTER I - FUNDAMENTAL DEFINITIONS AND THEOREMS

We begin our development of subdirect sums by recalling some of the basic concepts of the notion of direct sum.

Let S_i $(i = 1,2,\ldots)$ be rings, distinct or identical, and let

$$S = \dot{+}_i S_i = \{(s_1,s_2,\ldots) \mid s_i \in S_i \; i = 1,2,\ldots\}.$$

We define addition and multiplication as S as follows:

$$(s_1,s_2,\ldots) + (t_1,t_2,\ldots) = (s_1+t_1,s_2+t_2,\ldots)$$

$$(s_1,s_2,\ldots)(t_1,t_2,\ldots) = (s_1t_1,s_2t_2,\ldots).$$

S is called the direct sum of the rings S_i. It is easily verified that the direct sum of any set of rings is itself a ring and the zero of S is $(0,0,\ldots)$, the zero in the i^{th} place being the zero of S_i. Likewise, S has a unit element $(e_1,e_2,\ldots)$ if and only if e_i is the unit of S_i for all i.

It is to be noted that the direct sum notation does not imply that the number of rings S_i need be countable. The concept of direct sum does not depend on the cardinal number of $\{S_i\}$ nor on the fact that the set need be well ordered.

Lemma 1. Let

$$S_i' = \{(0,0,\ldots,0,s_i,0,\ldots) \mid s_i \in S_i\}.$$

Then $S_i' \subseteq S$ is a two sided ideal and $S_i' \cong S_i$ for all i.

Proof: Let $(0,0,\ldots,0,s_i,0,\ldots) \in S_i'$ and $(t_1,t_2,\ldots) \in S$.

Then

$$(0,\ldots 0,s_i,0,\ldots)(t_1,t_2,\ldots) = (0,\ldots,0,s_it_i,0,\ldots) \in S_i'$$

and

$$(t_1,t_2,\ldots)(0,\ldots 0,s_i,0,\ldots) = (0,\ldots 0,t_is_i,0,\ldots) \in S_i'.$$

It is clear that S_i' is a subgroup of the additive group of S. Hence S_i' is a two sided ideal in S.

Consider the correspondence

$$t_i \longleftrightarrow (0,\ldots,0,t_i,0,\ldots) \qquad t_i \in S_i$$

between S_i and S_i'. Clearly this correspondence is 1-1 and onto. If

$$s_i \longleftrightarrow (0,\ldots,0,s_i,0,\ldots) \qquad s_i \in S_i$$

then

$$s_i + t_i \longleftrightarrow (0,\ldots,0,s_i+t_i,0,\ldots) = (0,\ldots,0,s_i,0,\ldots) + (0,\ldots,0,t_i,0,\ldots)$$

and

$$s_it_i \longleftrightarrow (0,\ldots,0,s_it_i,0,\ldots) = (0,\ldots,0,s_i,0,\ldots)(0,\ldots,0,t_i,0,\ldots).$$

Thus the correspondence gives the desired isomorphism. Q.E.D.

We note that the correspondence

$$(s_1,s_2,\ldots) \longrightarrow (0,\ldots,0,s_i,0,\ldots)$$

defines a homomorphism of S onto S_i' with kernel n_i where

$$n_i = \left\{(s_1,\ldots,s_{i-1},0,s_{i+1},\ldots) \mid s_i \in S_i\right\}.$$

By the Fundamental Homomorphism Theorem we have

$$S/n_i \cong S_i' \cong S_i.$$

If the set of rings $\left\{S_i\right\}$ is finite, the direct sum will be denoted by

$$S = S_1 \dot{+} S_2 \dot{+} S_3 \dot{+} \ldots \dot{+} S_n.$$

Let $S = \dot{+}_{i\in I} S_i$ be the direct sum of the rings S_i, $i = 1,2,\ldots$ Let $T \subseteq S$ be a subring. If $t = (t_1,t_2,\ldots)$, $t_i \in S_i$ is an arbitrary element of T, then the correspondence

$$t \longrightarrow t_i$$

by the above and Lemma 1 defines a homomorphism of T into S_i as t varies over T, and hence onto a subring S_i^* of S_i. If for every $i \in I$, $S_i^* = S_i$, then T is called a <u>subdirect sum</u> of the rings S_i and each S_i is a <u>component</u> of T.

As an illustration of the above definition, let I/(2) and I/(4) denote the rings of integers modulo 2 and modulo 4 respectively. Then

$$S = I/(2) \dot{+} I/(4) = \{(\bar{0},\bar{0}),(\bar{0},\bar{1}),(\bar{0},\bar{2}),(\bar{0},\bar{3}),(\bar{1},\bar{0}),(\bar{1},\bar{1}),(\bar{1},\bar{2}),(\bar{1},\bar{3})\}$$

with the natural definitions of addition and multiplication. Let

$$T = \{(0,0),(1,1),(0,2),(1,3)\}.$$

Then $T \subset S$ and it is easily checked that it is a subring of S. Furthermore, T is a subdirect sum of I/(2) and I/(4) since every element of these rings is the image of some element of T under the correspondence defined in the definition above.

Let T be a subdirect sum of the rings S_i $(i = 1,2,\ldots)$. If a ring R is isomorphic to T, then T is a <u>representation</u> of R as a subdirect sum of the rings S_i $(i = 1,2,\ldots)$. Suppose the isomorphism between R and T is given by

$$r \longleftrightarrow t \qquad\qquad r \in R,\ t \in T.$$

Then the correspondence

$$r \longleftrightarrow t \longrightarrow t_i \qquad\qquad t_i \in S_i$$

defines a natural homomorphism of R onto S_i.

We are now able to state and prove the fundamental representation theorems on subdirect sums.

Theorem 1. A ring R is isomorphic to a subdirect sum T of rings S_i (i=1,2,...) if and only if there exist homomorphisms

$$h_i: R \longrightarrow S_i$$

such that if $r \in R$, $r \neq 0$, then $h_i(r) \neq 0$ for at least one i.

Proof: Let the isomorphism between R and T be given by

$$r \longleftrightarrow t .$$

Then the correspondence

$$r \longleftrightarrow t \longrightarrow t_i \qquad\qquad t_i \in S_i$$

defines a homomorphism

$$h_i: R \longrightarrow S_i \qquad (i=1,2,...).$$

Let $r \in R$, $r \neq 0$. Since $R \cong T$, $t \neq (0,0,...)$. Hence for some i, $t_i \neq 0$; i.e. for some i, $h_i(r) \neq 0$.

Now assume that there are homomorphisms

$$h_i: R \longrightarrow S_i$$

such that $h_i(r) \neq 0$ for some i when $r \neq 0$. The correspondence

$$r \longleftrightarrow (h_1(r), h_2(r), ...)$$

is one from R into the direct sum S of the rings S_i. We now show that this correspondence defines a homomorphism of R into S. Let $r,t, \in R$. Then since $h_i: R \longrightarrow S_i$ is a homomorphism we have

$$r+t \longrightarrow (h_1(r+t), h_2(r+t), ...) = (h_1(r)+h_1(t), h_2(r)+h_2(t), ...)$$
$$(h_1(r), h_2(r), ...) + (h_1(t), h_2(t), ...)$$

and

$$rt \longrightarrow (h_1(rt), h_2(rt), \ldots) = (h_1(r)h_1(t), h_2(r)h_2(t), \ldots)$$
$$= (h_1(r), h_2(r), \ldots)(h_1(t), h_2(t), \ldots).$$

Let $T = \{(h_1(r), h_2(r), \ldots) \mid r \in R\}$. Then since $h_i(r) \epsilon S_i$, $T \subseteq S$. Further, since the homomorphic image of a ring is a ring, T is a subring of S. Consider the correspondence

$$(h_1(r), h_2(r), \ldots) \longrightarrow h_i(r).$$

Since h_i is a homomorphism of R onto S_i, every element of S_i is the image of at least one element of R and hence of at least one element of T. Thus T is a subdirect sum of the rings S_i and the correspondence

$$r \longrightarrow (h_1(r), h_2(r), \ldots)$$

defines a homomorphism of R onto a subdirect sum of the rings S_i.

By the hypothesis if $r \in R$, $r \neq 0$, then $h_i(r) \neq 0$ for some i. Hence the above homomorphism has zero kernel and is in fact an isomorphism. Q.E.D.

Corollary: If R is homomorphic to each of a set of rings S_i^* and R is isomorphic to at least one of the S_i^*, then R has a representation as a subdirect sum of the rings S_i^*.

Proof: Let $h_i: R \longrightarrow S_i^*$ be a homomorphism for all i and for some i_o let $h_{i_o}: R \longrightarrow S_{i_o}^*$ be an isomorphism. Let $0 \neq r \in R$. Then $h_{i_o}(r) \neq 0$ and by Theorem 1, R is isomorphic to a subdirect sum of the rings S_i^*. Q.E.D.

If in a representation of R as a subdirect sum of rings S_i, the natural homomorphism of R onto S_i is an isomorphism for at least one i, then this is a trivial representation; otherwise it is a non-trivial representation of R.

Theorem 2. A ring R is isomorphic to a subdirect sum of rings S_i if and only if there exist in R two sided ideals J_i such that $R/J_i \cong S_i$ and $\bigcap_i J_i = 0$.

Proof: Suppose R is isomorphic to a subdirect sum of the rings S_i. By Theorem 1 for each i there exists a homomorphism $h_i: R \longrightarrow S_i$ such that if $0 \neq r \in R$, $h_i(r) \neq 0$ for some i. Let J_i designate the kernel of h_i. Then J_i is a two sided ideal in R and by the Fundamental Homomorphism Theorem

$$R/J_i \cong S_i.$$

Further, $\bigcap_i J_i = 0$. For suppose $0 \neq x \in \bigcap_i J_i$. Then $x \in J_i$ for all i and $h_i(x) = 0$ for all i which is a contradiction.

Conversely, suppose ideals J_i exist in R having the given properties. Then there exist homomorphisms $h_i: R \longrightarrow S_i$ with kernels J_i. If $h_i(r) = 0$ for all i, then $r \in \bigcap_i J_i$ and $r = 0$. Hence if $r \neq 0$, $h_i(r) \neq 0$ for some i and by Theorem 1, R is isomorphic to a subdirect sum of the rings S_i. Q.E.D.

It is seen that Theorems 1 and 2 are equivalent. Their principal contribution to the theory is in stating the main difficulty, that of establishing the existence of the required homomorphisms or ideals. It will be apparent that most of the results stated in this paper are applications of these theorems.

Let R be a ring and let J be a two sided ideal of R. J is said to be a prime ideal if for any $a,b \in R$, $ab \in J$ implies $a \in J$ or $b \in J$.

Lemma 2. If J is a prime ideal in a commutative ring R, then R/J is an integral domain.

Proof: R/J is a commutative ring so we need only show that

it has no divisors of zero. Let $\overline{a}$ be the residue class to which a belongs modulo J. Let $\overline{a},\overline{b} \in R/J$ be such that $\overline{ab} = 0$. Then $ab \equiv 0 \pmod{J}$ and hence $ab \in J$. Since J is prime, $a \in J$ or $b \in J$; i.e. $a \equiv 0 \pmod{J}$ or $b \equiv 0 \pmod{J}$. Hence $\overline{a} = 0$ or $\overline{b} = 0$. Q.E.D.

In the following, "ideal" will mean two sided ideal unless otherwise stated.

Let R be a commutative ring and J an ideal of R. A prime ideal $P \subsetneq R$ is a minimal prime ideal belonging to J if $J \subsetneq P$ and there does not exist a prime ideal $P' \subsetneq R$ such that $J \subsetneq P' \subset P$.

Let R be a commutative ring and J an ideal of R. Then we define the radical of J as follows:

$$\text{rad } J = \{r \in R \mid r^n \in J \text{ for some integer } n\}.$$

It can be shown that rad J is itself an ideal of R. The radical of a ring R is defined as the radical of the zero ideal.

Again let R be a commutative ring and $r \in R$. Then r is said to be nilpotent if $r^n = 0$ for some integer n. Thus we see that the radical of a commutative ring is simply the set of all nilpotent elements.

We state the following theorem without proof.

Theorem 3. The radical of an ideal J in a commutative ring R is the intersection of all minimal prime ideals belonging to J. (For proof see McCoy [12].)

Theorem 4. Let R be a commutative ring. Then R is isomorphic to a subdirect sum of integral domains if and only if R con-

tains no nonzero nilpotent element.

Proof: Let T be a subdirect sum of the integral domains T_i and let the isomorphism between R and T be given by

$$r \longleftrightarrow (t_1, t_2, \ldots) \qquad t_i \in T_i.$$

Then

$$r^k \longleftrightarrow (t_1^k, t_2^k, \ldots).$$

If $r^n = 0$ for some n, then $t_i^n = 0$ for all i since the above correspondence is an isomorphism. However, T_i is an integral domain and it contains no proper divisors of zero. Hence $t_i = 0$ for all i and r =0; i.e. R contains no nonzero nilpotent element.

Conversely, suppose R contains no nonzero nilpotent element. Then rad R = rad (0) = 0. Let

$$B = \left\{ q_i \mid q_i \text{ minimal prime ideal in R belonging to (0)} \right\}.$$

By Theorem 3, $\bigcap_i B = 0$. Let

$$A = \left\{ p_i \mid p_i \text{ prime ideal in R} \right\}.$$

Then $B \subseteq A$ and $\bigcap_i A \subseteq \bigcap_i B$. Hence $\bigcap_i A = 0$; i.e. the intersection of all prime ideals $p_i \subseteq R$ is zero. By Lemma 2 R/p_i is an integral domain and applying Theorem 2 we see that R is isomorphic to a subdirect sum of integral domains. Q.E.D.

CHAPTER II - SUBDIRECTLY IRREDUCIBLE RINGS

A ring R which has no non trivial representation as a subdirect sum of any set of rings is said to be <u>subdirectly irreducible</u>. Equivalently, R is <u>subdirectly reducible</u> if there exists a representation of R as a subdirect sum of rings S_i such that no one of the homomorphisms $R \longrightarrow S_i$ is an isomorphism.

We recall that a field F contains only two ideals, (0) and (F). There are, then, only two homomorphic images of F, $F/(0) \cong F$ and $F/F \cong (0)$. Suppose F is isomorphic to a subdirect sum of rings S_i. Not all the S_i can be zero, since F has more than one element. Hence, for some k, S_k is a field isomorphic to F. Thus no non trivial representation of F exists and F is subdirectly irreducible.

The following lemma follows immediately from Theorem 2.

<u>Lemma 3</u>. Let R be a ring and let B be the set of all nonzero ideals in R. Then R is subdirectly irreducible if and only if $\bigcap B \neq (0)$.

<u>Proof</u>: Suppose R is subdirectly reducible. Then R has a non trivial representation as a subdirect sum of rings S_i; i.e. there exists nonzero ideals $a_i \subseteq R$ such that $\bigcap \{a_i\} = (0)$ and $R/a_i \cong S_i \not\cong R$ for any i. If $A = \{a_i\}$, then $\bigcap B \subseteq \bigcap_i A = (0)$.

Suppose a_i are nonzero ideals in R such that $\bigcap_i \{a_i\} = (0)$ and $R/a_i \cong S_i$. By Theorem 2 a non trivial representation of R as a subdirect sum of rings exists and R is subdirectly

reducible. Hence if R is subdirectly irreducible we can not find a set of nonzero ideals in R with zero intersection; i.e. $\bigcap B \neq (0)$. Q.E.D.

We note, then, that $J = \bigcap B \neq (0)$ is the unique minimal ideal in a subdirectly irreducible ring.

The following fundamental theorem shows the importance of subdirectly irreducible rings in the theory of subdirect sums.

Theorem 5. Any ring R is isomorphic to a subdirect sum of subdirectly irreducible rings.

Before proving this theorem we recall the following facts. Let $\mathcal{M}$ be a set and $\mathcal{L}$ a collection of subsets of $\mathcal{M}$. If $M \in \mathcal{L}$ is such that if $M \subseteq A$ for any $A \in \mathcal{L}$ implies $M = A$, then M is said to be a maximal element in $\mathcal{L}$. Let $\mathcal{M}$ and $\mathcal{L}$ be as above. If for any L_i, $L_j \in \mathcal{L}$, $L_i \subseteq L_j$ or $L_j \subseteq L_i$, then $\mathcal{L}$ is said to be totally ordered with respect to inclusion.

Zorn's Lemma. Let $\mathcal{M}$ be a set and $\mathcal{L}$ a collection of subsets of $\mathcal{M}$. If the union of any totally ordered subcollection of $\mathcal{L}$ is an element of $\mathcal{L}$, then $\mathcal{L}$ has a maximal element.

Proof of Theorem 5: Let $0 \neq a \in R$ and let

$$\mathcal{L} = \{J \mid J \text{ an ideal of } R \text{ and } a \notin J\}.$$

Then $(0) \in \mathcal{L}$. Further, since the union of a totally ordered set of ideals not containing a is an ideal not containing a, we have that if $L_\alpha \in \mathcal{L}$ for $\alpha \in \mathcal{U}$, then

$$\bigcup_{\alpha \in \mathcal{U}} L_\alpha \in \mathcal{L}.$$

By Zorn's Lemma there exists a maximal ideal $J_a \in \mathcal{L}$. Now

suppose

$$0 \neq x \in \bigcap \{J_a \mid a \in R,\ a \neq 0\}.$$

Then $x \in J_a$ for all $a \in R$, $a \neq 0$ and hence $x \in J_x$. This is a contradiction. Thus

$$\bigcap \{J_a \mid a \in R,\ a \neq 0\} = (0).$$

By Theorem 2, R is isomorphic to a subdirect sum of the rings R/J_a.

We now show that R/J_a is subdirectly irreducible for each $a \in R$, $a \neq 0$. Let $\bar{x}$ denote the residue class to which x belongs modulo J_a. Since $a \notin J_a$, $a \not\equiv 0 \pmod{J_a}$ and hence $\bar{a} \neq 0$. Let N be any nonzero ideal of R/J_a and let

$$K = \{r \in R \mid \bar{r} \in N\}.$$

Then it is clear that K is an ideal of R and $J_a \subseteq K$. If $J_a = K$, $N = 0$ which is impossible. Thus $J_a \subset K$ and since J_a is maximal in $\mathcal{L}$, $K \notin \mathcal{L}$. Hence $a \in K$, $\bar{a} \in N$ and $\bar{a} \neq 0$. Hence we have

$$\bigcap \{(0) \neq N \mid N \text{ an ideal of } R/J_a\} \neq (0)$$

and by Lemma 3, R/J_a is subdirectly irreducible for each $a \in R$, $a \neq 0$. Q.E.D.

A simple ring R is a ring which has no nonzero two sided ideals except R itself. From Lemma 3, we have immediately the following theorem.

Theorem 6. A simple ring is subdirectly irreducible.

G. Birkhoff [1] was the first to prove the following result.

Theorem 7. A subdirectly irreducible commutative ring R with no nonzero nilpotent elements is a field.

Proof: By Lemma 3 there is an element j of R, $j \neq 0$ such that j is in all nonzero ideals of R. Let

$$J = \{yj^2 \mid y \in R\}.$$

Then it is clear that J is an ideal and $j^3 \in J$. Since R is without nonzero nilpotent elements, $j^3 \neq 0$. Thus $J \neq (0)$ and hence $j \in J$; i.e. there exists $x \in R$ such that $xj^2 = j$. If $e = xj$, then

$$e^2 = x^2j^2 = x(xj^2) = xj = e$$

and $e \neq 0$ since

$$ej = xj^2 = j \neq 0.$$

We also note that any ideal of R containing j must also contain e since $e = xj$ and $x \in R$. Thus e is in all nonzero ideals of R. Let

$$L = \{t\text{-}te \mid t \in R\}.$$

It is clear that L is an ideal in R. If $L \neq (0)$, $e \in L$ and for some $t_1 \in R$

$$e = t_1\text{-}t_1e.$$

Then

$$e^2 = t_1e\text{-}t_1e^2 = t_1e\text{-}t_1e = 0,$$

implies that $e = 0$ since R has no nonzero nilpotent elements. This is a contradiction. Hence $L = (0)$, and $t = te$ for all $t \in R$ and e is the unit of R. Since e is in all nonzero ideals of R, the ring must be simple.

Let $a \in R$, $a \neq 0$ and let $B = \{ax \mid x \in R\}$. Since B is an ideal and $a^2 \neq 0$ is in B, $B = R$. Hence the equation $ax = b$ has a unique solution x for each $b \in R$; i.e. R is a field.

Commutative subdirectly irreducible rings are completely characterized by the following result due to McCoy [10].

Theorem 8. Let R be a commutative ring with at least one element which is not a divisor of zero and let D be the set of all divisors of zero in R. Then R is subdirectly irreducible if and only if it has the following properties:

1) $J = \{x \in R \mid Dx = 0\}$ is a principal ideal $J = (j) \neq (0)$;

2) $D = \{y \in R \mid Jy = 0\}$;

3) R/D is a field;

4) If $d_1 \in D$ and $d_1 \notin J$, then there exists $d_2 \in D$, $d_2 \notin J$ such that $d_1 d_2 \in J$.

Proof: If R has no nilpotent elements and is subdirectly irreducible, by Theorem 7 R is a field and D = (0). Thus J =R=(e) where e is the identity of R. Clearly R/(0) is a field and Jy = 0 if and only if y = 0. Property 4) does not apply here. Conversely, suppose R has the stated properties and is without nilpotent elements. If $D \neq (0)$, there exists a $d_1 \in D$, $d_1 \neq 0$. Since jD = 0 and $j \neq 0$ we have $jd_1 = 0$; i.e. $j \in D$. Again, since jD = 0 and $j \in D$, $j^2 = 0$. This is a contradiction. Hence D = (0)and $R/(0) \cong R$ is a field and thus is subdirectly irreducible. We have shown that the theorem is true when R is without nilpotent elements.

Assume, now, that R has at least one nilpotent element and that R satisfies the stated properties. We first show that $J \subseteq (a)$ for all $a \neq 0$.

$$J = (j) = \{rj+nj \mid r \in R, \text{ n an integer}\} .$$

First suppose $a \in J$, $a \neq 0$. Then

$$a = bj+kj$$

for some $b \in R$, k an integer. Let $c \in R$, $c \notin D$. Then

$$ac = (bj+kj)c = (bc+kc)j \neq 0.$$

By property 2) J annihilates all of D so that $bc+kc \notin D$. Let $\overline{x}$ denote the residue class to which x belongs modulo D. Then $\overline{bc+kc} = 0$. By property 3) there exists $\overline{x} \in R/D$ such that

$$\overline{x}(\overline{bc+kc}) = \overline{1}$$

where $\overline{1}$ is the unit of R/D. Then for any $\overline{y} \in R/D$

$$\overline{x}(\overline{bc+kc})\overline{y} = \overline{y}.$$

Hence

$$x(bc+kc)y = y+d$$

for some $d \in D$ depending on y. Letting $y = c$ we have

$$x(bc+kc)cj = cj+dj = cj$$

since $jD = 0$. Since $c \notin D$ we have

$$x(bc+kc)j = j$$

and

$$axc = (bj+kj)xc = j.$$

Thus $j \in (a)$ and hence $J \subseteq (a)$.

If $a \in D$, $a \notin J$, then by 4) there exists $d_1 \in D$, $d_1 \notin J$ such that $j = ad_1$; i.e. $J \subseteq (a)$.

Now if $a \notin D$, then $\overline{a} = 0$ and there exists $\overline{x} \in R/D$ such that $\overline{ax} = \overline{1}$, where $\overline{1}$ is as above. Then $\overline{axa} = \overline{a}$ or equivalently

$$axa = a+d$$

for some $d \in D$. Further, since $axaj = aj+dj = aj$ and $a \in D$

$$axj = j$$

and $J \subseteq (a)$. Thus the intersection of all nonzero ideals in R is not zero and Lemma 3 gives one part of the theorem.

Now suppose that R has at least one nilpotent element and is subdirectly irreducible. By the remark preceeding Theorem 5, R has a unique minimal ideal $J \neq (0)$. If $a \in J$, $a \neq 0$, then $(a) \subseteq J$ by definition of the principal ideal. Since J is minimal, $(a) = J$; i.e. J is generated by any one of its nonzero elements. Suppose $J = (j)$, $0 \neq j \in J$.

Let $0 \neq a \in R$ be arbitrary. Then since $R \neq D$, $aR \neq (0)$ and aR is an ideal in R. Hence $J \subseteq aR$ and there exists $x \in R$ such that

$$ax = j. \qquad (I)$$

Recall that the radical of R is an ideal and so it contains J; i.e. j is nilpotent. Suppose $j^2 \neq 0$. From above $j^2 y = j$ for some $y \in R$ and $j^3 y = j^2 \neq 0$ implies $j^3 \neq 0$. We see that if $j^2 \neq 0$, $j^n \neq 0$ for any integer n. This is a contradiction since j is nilpotent. Thus $j^2 = 0$ necessarily.

Let $a \in R$ be arbitrary and consider the ideal aJ. Either $aJ = (0)$ or $J \subseteq aJ$. But it is clear that $aJ \subseteq J$ and thus either $aJ = (0)$ or $aJ = J$. Clearly if $a \notin D$, $aJ = J \neq 0$; i.e.

$$\{y \in R \mid yJ = 0\} \subseteq D.$$

Now let

$$B = \{x \in R \mid ax = 0\}.$$

Then B is an ideal in R and either $B = (0)$ or $J \subseteq B$. If $a \in D$, then $B \neq (0)$ and $J \subseteq B$. Hence $aJ \subseteq aB = (0)$. Thus $aJ = 0$and

$$D = \{y \in R \mid yJ = 0\}$$

which is property 2) of the theorem.

We now show that R/D is a field. Suppose $a \in R$ and $c \notin D$ are arbitrary. Then $cj \neq 0$ and from above there exists $x \in R$ such that $cjx = j$. Thus $cjxa-ja = (cxa-a)j = 0$ and $cxa-a \in D$. Let $y = xa$. Then $cy-a \equiv 0 \pmod{D}$ or equivalently

$$\overline{cy} = \overline{a}.$$

Since $a \in R$ and $c \notin D$ were arbitrary, this shows that R/D is a field.

We now consider property 1). Let $0 \neq a \in R$ be such that $aD = 0$. From equation (I) above there exists $x \in R$ such that $ax = j$. If $c \notin D$, then

$$axc = cj \neq 0$$

and thus $xc \notin D$; i.e. $\overline{xc} \neq 0$. By property 3) there exists $\overline{t} \in R/D$ such that $\overline{xct} = \overline{c}$, or equivalently

$$xct = c+d$$

for some $t \in R$, $d \in D$. From above we have, since $ad = 0$

$$axct = a(c+d) = ac+ad = ac = cjt .$$

Hence $a = jt$ and $a \in J$. Thus

$$\{x \in R \mid xD = 0\} \subseteq J.$$

But, since J is minimal

$$J \subseteq \{x \in R \mid xD = 0\}$$

and property 1) is established.

Let $d_1 \in D$, $d_1 \notin J$. Then by equation (I) $d_1d_2 = j \in J$ for some $d_2 \in R$. If $d_2 \in J$, by property 2), $d_1d_2 = 0$ which is a contradiction since $j \neq 0$. Hence $d_2 \notin J$. If $d_2 \notin D$, then since

$$jD = d_1d_2D = 0$$

by property 1) we must have $d_1D = 0$. Again property 1) implies that $d_1 \in J$ which is a contradiction. Thus $d_2 \in D$ and this completes the proof.

Corollary. Let I be the integers and p a prime. Then $R = I/(p^m)$ is subdirectly irreducible.

Proof: Clearly R is a commutative ring with a unit and D is not empty. Let $\bar{x} \in D$. Then there exists $\bar{y} \in R$, $\bar{y} \neq 0$ such that $\overline{xy} = 0$; i.e. $xy \equiv 0 \pmod{(p^m)}$. Thus $p \mid xy$ ("p divides xy") and hence $p \mid x$ or $p \mid y$. Suppose the latter is the case. Then $\bar{y} = \overline{kp}$ for some $\bar{k} \in R$ and since $\overline{xy} = 0$ we must have $\bar{x} = \overline{mp^{m-1}}$ for some $\bar{m} \in R$; i.e. $\bar{x} \in (\bar{p})$. If $p \mid x$, then clearly $\bar{x} \in (\bar{p})$. Hence $D \subseteq (\bar{p})$.

Now suppose $0 = \bar{x} \in (\bar{p})$. Then $\bar{x} = \overline{lp}$ for some $\bar{l} \in R$. Letting $\bar{y} = \overline{np^{m-1}}$, $\bar{n} \in R$, we have $\bar{y} = 0$ and $\overline{xy} = \overline{lnpp^{m-1}} = 0$; i.e. $\bar{x} \in D$ and $(\bar{p}) \subseteq D$. Thus $D = (\bar{p})$. Observe that we have also shown $J = (\overline{p^{m-1}})$.

To show that $R/(\bar{p})$ is a field, we need only show that $(\bar{p})$ is maximal in R. Suppose A is an ideal of R such that $(\bar{p}) \subset A$. Then there exists $\bar{x} \in A$, $\bar{x} \notin (\bar{p})$ and the greatest common divisor of x and p must be one. Hence there exist integers s and t such that $sx+tp = 1$, or equivalently

$$\overline{sx} + \overline{tp} = \bar{1}.$$

Since A is an ideal and $\bar{p} \in A$, $\bar{1} \in A$. Thus $A = R$, and $(\bar{p})$ is maximal in R; i.e. $R/(\bar{p})$ is a field.

Finally, let $\bar{d}_1 \in D$, $\bar{d}_1 \notin J$. Then $\bar{d}_1 = \overline{yp}$ for some $\bar{y} \notin J$.

If $m > 2$, let $\overline{d}_2 = \overline{zp}^{m-2}$. Then $\overline{d}_2 \in (\overline{p}) = D$ and $\overline{d}_2 \notin J$. Also,

$$\overline{d_1 d_2} = \overline{yzp}^{m-2}\overline{p} = \overline{yzp}^{m-1} \in J.$$

If $m \leq 2$, then $J = (\overline{p})$ or $J = R$ and there is no element of D not in J.

Q.E.D.

The representation of a ring R as a subdirect sum of subdirectly irreducible rings is not unique. Let I be the integers and let p_k be a prime of the form 4n-1. If $A = \bigcap_k \{(p_k)\}$, then A = (0). For if not, there is an $x \neq 0$ such that x is indivisible by all primes of the form 4k-1. Clearly this is an impossibility. By Theorem 2 I is isomorphic to a subdirect sum of the fields $I/(p_k)$ each of which is subdirectly irreducible. Similarly, if q_k is a prime of the form 4j+1 and if $B = \bigcap_k \{(q_k^2)\}$, then B = (0) and I is isomorphic to a subdirect sum of the rings $I/(q_k^2)$ each of which is subdirectly irreducible by the above Corollary. Note, however, that since (q_k^2) is contained in (q_k), (q_k^2) is not maximal and thus $I/(q_k^2)$ is not a field. Hence these two representations are essentially different.

CHAPTER III - CHARACTERIZATIONS OF P-RINGS AND REGULAR RINGS

A Boolean ring is a ring R of more than one element in which each element is idempotent; i.e.

$$x^2 = x$$

for all $x \in R$.

Lemma 4. A Boolean ring R has characteristic 2 and is commutative.

Proof: Let $a \in R$ be arbitrary. Then $a^2 = a$. Since $2a \in R$,

$$(2a)^2 = 4a^2 = 4a = 2a$$

and thus $2a = 0$. Note then that $a = -a$ for all $a \in R$.

Let $a, b \in R$. Then $a + b \in R$ and

$$a+b = (a+b)^2 = a^2+ab+ba+b^2 = a+ab+ba+b.$$

Hence $ab + ba = 0$ and $ab = -ba = ba$ from above. Q.E.D.

Since $x^2 = x$, it is clear that $x^k = x$ for any integer k and thus a Boolean ring can have no nonzero nilpotent elements.

We can now easily prove the following result first formulated by M.H. Stone [14].

Theorem 9. Aring R is a Boolean ring if and only if it is isomorphic to a subdirect sum of fields I/(2).

Proof: Suppose R is isomorphic to a subdirect sum T of fields I/(2). Clearly R is a ring with more than one element. If

$$t = (t_1, t_2, \ldots) \in T$$

where $t_i \in I/(2)$ we have

$$t^2 = (t_1^2, t_2^2, \ldots) = (t_1, t_2, \ldots) ;$$

i.e. each element of T is idempotent. Hence each element of R is idempotent and R is Boolean.

Conversely, suppose R is Boolean. By Theorem 5 R is isomorphic to a subdirect sum of subdirectly irreducible rings S_i. Thus each S_i is a homomorphic image of R. We now show that if $S_i \neq 0$, then S_i is a Boolean ring. Suppose

$$h_i : R \longrightarrow S_i$$

is a homomorphism. Then for any $r \in R$,

$$[h_i(r)]^2 = [h_i(r)][h_i(r)] = h_i(r^2) = h_i(r) \ ;$$

i.e. each S_i is a subdirectly irreducible Boolean ring. Since a Boolean ring is commutative with more than one element and zero radical, by Theorem 7 we have that each S_i is a field. Moreover, each S_i has characteristic 2 and each element satisfies the equation $x^2-x = 0$. Hence $S_i = I/(2)$. Q.E.D.

Let p be a fixed prime. Then a ring R with more than one element is a <u>p-ring</u> if

$$x^p = x \qquad \text{and} \qquad px = 0$$

for each $x \in R$. Note that a Boolean ring is a p-ring with p=2.

It has been shown by McCoy [12] that a p-ring is necessarily commutative. As in the case of a Boolean ring, a p-ring can have no nonzero nilpotent elements. McCoy and Montgomery [8] have generalized the preceding theorem as follows.

<u>Theorem 10</u>. A ring R is a p-ring if and only if it is isomorphic to a subdirect sum of fields I/(p).

<u>Proof</u>: Assume R is a p-ring. By Theorem 5, R is isomorphic to a subdirect sum of subdirectly irreducible rings S_i, each

of which must be a commutative p-ring since each S_i is the homomorphic image of a commutative p-ring. Thus each S_i is a field. Further,

$$x^p = x \qquad \text{and} \qquad px = 0$$

for each $x \in S_i$ $i = 1,2,\ldots$. Hence each S_i is isomorphic to $I/(p)$.

Now let T be a subdirect sum of the fields $I/(p)$ and let

$$h: R \longleftrightarrow T$$

be an isomorphism. If $t \in T$, then there exists $r \in R$ such that $h^{-1}(t) = r$. Recall, if $t_i \in I/(p)$, $t_i^p = t_i$ and $pt_i = 0$. Hence, since $h^{-1}: T \longleftrightarrow R$ is also an isomorphism,

$$r^p = [h^{-1}(t)]^p = h^{-1}(t^p) = h^{-1}(t) = r$$

and

$$pr = ph^{-1}(t) = h^{-1}(pt) = h^{-1}(0) = 0.$$

Clearly, R has more than one element and thus R is a p-ring.

Q.E.D.

The concept of a regular ring is due primarily to J. von Neumann [15]. A ring R is <u>regular</u> if for each $a \in R$ there exists an $x \in R$ such that

$$axa = a.$$

Note that the existence of a unit element is not assumed.

A <u>division ring</u> R is a ring with more than one element and in which the equation

$$ax = b$$

has a unique solution x in R for each $a, b \in R$, $a \neq 0$. We note that a division ring R has no proper divisors of zero. For suppose $c, d \in R$ $c \neq 0$, $d \neq 0$. Then there exists

elements x and y in R such that

$$cx = d \qquad \text{and} \qquad dy = x.$$

Then

$$cdy = cx = d \neq 0$$

and thus $cd \neq 0$.

Lemma 5. Every division ring D has a unit element.

Proof: Let $0 \neq a \in D$ and $0 \neq e \in D$ be such that $ae = a$. Then $ae^2 = ae$ implies that

$$a(e^2-e) = 0.$$

Since $a \neq 0$ and D has no proper divisors of zero we must have

$$e^2 = e.$$

Let $t \in D$ be arbitrary. Then

$$(t-te)e = te-te^2 = te-te = 0$$

and

$$e(t-et) = et-e^2t = et-et = 0.$$

Since $e \neq 0$ and D has no proper divisors of zero we must have

$$t-te = t-et = 0$$

i.e.

$$t = et = te.$$

Hence e is the unit element of D. Q.E.D.

Since every nonzero element of a division ring has an inverse, it is easily seen that such a ring must be regular. Observe that a p-ring R is regular. For let $a \in R$ and suppose $p > 2$. Then

$$aa^{p-2}a = a^p = a.$$

If $p = 2$, then

$$aaa = a^2a = a^2 = a.$$

The center C(R) of a ring R is defined as follows.

$$C(R) = \{r \in R \mid ra = ar \text{ for all } a \in R\}.$$

The following lemmas and theorem are due to A. Forsythe and McCoy [3].

Lemma 6. Let R be a ring without nonzero nilpotent elements. Then every idempotent of R is in C(R).

Proof: Let $c \in R$ be idempotent and let $x \in R$ be arbitrary. Then

$$(cxc-cx)^2 = cxc^2xc-cxccx-cxcxc + cxcx$$

$$= cxcxc-cxcx-cxcxc + cxcx = 0.$$

Since R has no nonzero nilpotent elements, cxc = cx. Similarly cxc = xc. Hence cx = xc for all $x \in R$; i.e. $c \in C(R)$.

Lemma 7. If R is a subdirectly irreducible ring without nonzero nilpotent elements, then the only idempotents in R are the zero and the unit if the latter exists.

Proof: Suppose c is idempotent, $c \neq 0$. By Lemma 6 $c \in C(R)$. Let $J = \{x-cx \mid x \in R\}$. Then since $c \in C(R)$, it is clear that J is an ideal in R. If J = (0), x = cx = xc for all $x \in R$; i.e. R has a unit element c. If $J \neq (0)$, let

$$L = \{cx \mid x \in R\}.$$

Then L is an ideal in R because of Lemma 6 and since $c^2 \in L$, $c^2 = c \neq 0$, $L \neq (0)$. If $z \in J \cap L$, then there exist $x, y \in R$ such that

$$z = x-cx = cy.$$

Then

$$z = cy = c(cy) = c(x-cx) = cx-cx = 0$$

and $J \cap L = (0)$. Thus the intersection of all nonzero ideals in R is zero and by Lemma 3 R is not subdirectly irreducible.

Lemma 8. A regular ring R has no nonzero nilpotent elements if and only if for each $a \in R$ there exists $x \in R$ such that $a^2x = a$.

Proof: Suppose R is regular and without nonzero nilpotent elements. Let $a \in R$. Then there exists $x \in R$ such that $axa = a$. Since

$$(ax)^2 = axax = ax$$

ax is idempotent and by Lemma 6 $ax \in C(R)$. Thus

$$a = axa = aax = a^2x.$$

Conversely, suppose $a \neq 0$ and $a^2x = a$ for some $x \in R$. Then $a^2 \neq 0$ and $a^3x^2 = a^2x = a \neq 0$. Hence $a^3 \neq 0$. It is easily seen that $a^n \neq 0$ for any integer n. Q.E.D.

The following theorem due to A. Forsythe and McCoy [3] characterizes regular rings in terms of division rings.

Theorem 11. Let R be a regular ring. Then R is isomorphic to a subdirect sum of division rings if and only if R has no nonzero nilpotent elements.

Proof: Suppose R is isomorphic to a subdirect sum T of division rings D_i and that the correspondence is given by

$$r \longleftrightarrow (d_1, d_2, \ldots) \qquad d_i \in D_i.$$

If $r \in R$ is nilpotent, then $r^n = 0$ for some n. Hence

$$(d_1^n, d_2^n, \ldots) = 0$$

Since a division ring has no proper divisors of zero, we must have $d_i = 0$ for all i; i.e. $r = 0$. Note that this proof of the necessity of the condition did not use the fact that R is regular.

Now let R be a regular ring with no nonzero nilpotent elements. By Theorem 5, R is isomorphic to a subdirect sum of subdirectly irreducible rings D_i. Each D_i is a homomorphic image of the ring R and is therefore regular. For let

$$h_i : R \longrightarrow D_i$$

be a homomorphism. Then for each $a \in R$ there exists $x \in R$ such that $axa = a$. Thus, since

$$h_i(a)h_i(x)h_i(a) = h_i(a)$$

and h_i is onto for each i, D_i is regular. Also, by Lemma 8 for each $a \in R$ there exists $x \in R$ such that $a^2x = a$. Hence for each h_i

$$h_i(a^2x) = [h_i(a)]^2 h_i(x) = h_i(a).$$

Since h_i is onto, Lemma 8 implies that D_i has no nonzero nilpotent elements. By Lemma 7 the only idempotents in D_i are the zero and the unit if the latter exists. Let $d_i \in D_i$, $d_i \neq 0$. Then there exists $x_i \in D_i$ such that

$$d_i x_i d_i = d_i \neq 0.$$

Thus $d_i x_i \neq 0$ and

$$(d_i x_i)^2 = d_i x_i d_i x_i = d_i x_i ;$$

i.e. $d_i x_i$ is idempotent and $d_i x_i = e_i$ where e_i is the unit of D_i, the existence of which was demonstrated in Lemma 5. Similarly, $x_i d_i \neq 0$ and is idempotent. Hence $x_i d_i = e_i$. Since every nonzero element of D_i has an inverse, D_i is a division ring for each i.

Q.E.D.

CHAPTER IV - SUBDIRECT SUM REPRESENTATIONS OF PRIME RINGS

In the preceding chapters we were concerned with conditions under which a given ring is isomorphic to a subdirect sum of rings of a certain type. Krull [7] was the first to contribute significantly to a solution of the converse problem. He took a set of fields and examined the various subdirect sums of this set to determine which, if any, were representations of an integral domain. In his early work he placed restrictions on the given set of rings which of course limited his results. McCoy [11] has since weakened many of Krull's hypotheses and generalized the results to a larger class, that of prime rings.

We shall first discuss prime rings and prove some theorems needed in the sequel. The notion of prime ideal can be generalized as follows. Let R be a ring and let P be an ideal of R. Let A, B be any ideals of R. P is <u>prime</u> if $AB \equiv 0 \pmod{P}$ implies $A \equiv 0 \pmod{P}$ or $B \equiv 0 \pmod{P}$. A <u>ring</u> R is <u>prime</u> if (0) is a prime ideal of R. It is not difficult to show that R/P is prime if and only if P is prime in R.

<u>Lemma 9</u>. Let R be a ring and $a_1, a_2, \ldots, a_n \in R$. If (0) is prime and $(a_1)(a_2)\ldots(a_n) = (0)$, then $(a_i) = (0)$ for some i, $1 \leq i \leq n$.

<u>Proof</u>: We prove this lemma by induction on n. If $n = 2$, the lemma is trivial by definition of (0) being prime. Suppose it is true for some k, $2 \leq k \leq n-1$. If $(a_1)\ldots(a_{k+1}) = (0)$,

then for any $\bar{a}_i \in (a_i)$, since $\bar{a}_1 \ldots \bar{a}_k \in (a_1)(a_2)\ldots(a_k)$, we have

$$(\bar{a}_1 \ldots \bar{a}_k)(a_{k+1}) \subseteq (a_1)(a_2)\ldots(a_{k+1}) = 0.$$

Hence $(\bar{a}_1 \ldots \bar{a}_k) = 0$ or $(a_{k+1}) = 0$. If the latter case, we are done. So suppose $(\bar{a}_1 \ldots \bar{a}_k) = 0$. Then $\bar{a}_1 \ldots \bar{a}_k = 0$ for any $a_i \in (a_i)$, $1 \leq i \leq k$. Hence $(a_1)(a_2)\ldots(a_k) = 0$ and $a_i = 0$ for some i, $1 \leq i \leq k$ by the inductive hypothesis. Q.E.D.

Theorem 12. A ring R is prime if and only if for arbitrary $a, b \in R$, if $aRb = 0$, then $a = 0$ or $b = 0$.

Proof: Assume the condition on the statement of the theorem. Let A, B be ideals of R and suppose $AB = 0$ and $B \neq 0$. Since $RB \subseteq B$ and $ARB \subseteq AB = 0$, $ARB = 0$. Since $B \neq 0$, there exists $b \in B$, $b \neq 0$. Let $a \in A$ be arbitrary. Then $(a) \subseteq A$, $(b) \subseteq B$ and hence

$$(a)R(b) \subseteq ARB = 0.$$

Since $aRb \subseteq (a)R(b) = 0$, $aRb = 0$. By the condition, $a = 0$ since $b \neq 0$. Since $a \in A$ is arbitrary, $A = 0$; R is prime.

Conversely, suppose R is prime and $aRb = 0$. Then $RaRbR = 0$. By a straight forward calculation it can be verified that

$$(a)^2(b)^3 \subseteq RaRbR = 0$$

and by Lemma 9 $(a) = 0$ or $(b) = 0$; i.e. $a = 0$ or $b = 0$. Q.E.D.

Recall that C(R) denotes the center of the ring R. Let N(R) designate the cardinality of C(R). We make the convention that if C(R) is infinite $N(R) = \infty$; otherwise, N(R) is a positive integer. Note that if $N(R) = 1$, $C(R) = 0$. In the

following we shall be concerned only with rings R such that $N(R) > 1$.

It is clear that a commutative prime ring is an integral domain since it can have no proper divisors of zero.

Lemma 10. A finite integral domain is a field.

Proof: Let the finite integral domain D have n distinct elements $a_1, a_2, \ldots a_n$. Let $a \neq 0$ be any element of D and consider the n products

$$aa_1, aa_2, \ldots aa_n.$$

These must all be distinct for if

$$aa_i = aa_j$$

we must have

$$a(a_i - a_j) = 0$$

and since D has no divisors of zero and $a \neq 0$, $a_i = a_j$ which is a contradiction.

Thus the n products aa_i, $1 \leq i \leq n$ give all the elements of D. Hence for any $b \in D$ there exists a unique $a_i \in D$ such that

$$aa_i = b.$$

Thus D is a division ring and since it is commutative, D is a field. Q.E.D.

Theorem 13. If R is a prime ring, then C(R) contains no proper divisors of zero and if $1 < N(R) < \infty$, C(R) is a finite field.

Proof: Let $c \in C(R), c \neq 0$, and $r \in R$. Suppose $cr = rc = 0$. We first show that $(c)(r) = 0$. Since

$(c) = \{nc+r'c \mid n\in I,\ r'\in R\}$ and $(r) = \{jr+\bar{r}r+r'' \mid j\in I, \bar{r}, r''\in R\}$

we have

$$(c)(r) = \{\sum(nc+r'c)(jr+\bar{r}r+r''r)\} = \{\sum(ncjr+nc\bar{r}r+ncr''r + r'cjr+r'c\bar{r}r+r'cr''r)\}$$

$$= \{\sum(njcr+n\bar{r}cr+nr''cr+jr'cr+r'\bar{r}cr+r'r''cr)\} = 0$$

since $cr = 0$. Since R is prime, $(c) = 0$ or $(r) = 0$. Hence $\bar{r} = 0$ since $(c) \neq 0$; i.e. R has no proper divisors of zero.

Clearly, C(R) is a commutative ring. Let A, J be ideals of C(R). Assume $A \neq (0)$ and $AJ = (0)$. Then there exists $a \in A$, $a \neq 0$ and further for all $j \in J$, $aj = 0$. By the above since $a \neq 0$ we must have $j = 0$ for all $j \in J$; i.e. $J = (0)$. Thus C(R) is a prime ring and hence is an integral domain. If $1 < N(R) < \infty$, C(R) is a finite integral domain and hence a field by the previous lemma. Q.E.D.

Theorem 14. If R is a prime ring and x an indeterminate, then the polynomial ring R[x] is prime.

Proof: Let f(x) and g(x) be polynomials of degrees m and n respectively. If $f(x)R[x]g(x) = 0$, then in particular

$$f(x)Rg(x) = 0.$$

Suppose $f(x) \neq 0$ and let a_k be the first nonzero coefficient of f(x). Then

$$f(x)Rg(x) = (a_kx^k + a_{k+1}x^{k+1}+\ldots a_mx^m)R(b_o + b_1x +\ldots+b_nx^n)$$
$$= (a_kRb_o)x^k + (a_{k+1}Rb_o + a_kRb_1)x^{k+1} +$$
$$(a_kRb_2 + a_{k+1}Rb_1 + a_{k+2}Rb_o)x^{k+2}+\ldots+(a_mRb_n)x^n$$
$$= 0$$

and thus all coefficients must be zero; i.e.

$$a_k Rb_o = a_{k+1} Rb_o + a_k Rb_1 = \ldots a_m Rb_n = 0.$$

Since R is prime and $a_k \neq 0$, Theorem 12 implies that $b_i = 0$ $i = 0,1,2,\ldots,n$; i.e. $g(x) = 0$. The same theorem also then implies that R[x] is prime. Q.E.D.

Theorem 15. A prime ring R without a unit can be imbedded in a prime ring T with a unit and $C(R) \subseteq C(T)$.

Proof: Let $T = R + I/(2)$. Then for $(r_1,a),(r_2,b) \in T$ define

$$(r_1,a) + (r_2,b) = (r_1+r_2,\ a+b)$$

$$(r_1,a)(r_2,b) = (r_1r_2 + ar_2 + br_1,\ ab).$$

T has the element (0,1) as a unit. It is easily verified that T is prime. Let

$$S = \{(r,0) \mid r \in R\}.$$

Then S is a subring of T and the correspondence

$$r \longleftrightarrow (r,0)$$

clearly defines an isomorphism between R and S. Thus R is imbedded in T.

Further, for any $(r,a) \in T$ and $r' \in C(R)$ we have

$$(r',0)(r,a) = (r'r + ar',0) = (rr' + r'a,0) = (r,a)(r',0).$$

Hence, $(r',0) \in C(T)$ and $C(R) \subseteq C(T)$. Q.E.D.

The following theorem will be useful for future results.

Theorem 16. Let R be a prime ring and x an indeterminate. If $f(x) \in R[x]$ is of degree n, then there exist at most n elements $a_i \in C(R)$ such that $f(a_i) = 0$.

Proof: Suppose R has a unit and $a_1 \in C(R)$. By the Remainder Theorem we may write

$$f(x) = g(x)(x-a_1) + f_R(a_1), \qquad f(x) = (x-a_1)k(x) + f_L(a_1)$$

where $f_R(a_1)$ and $f_L(a_1)$ are the unique right and left remainders of $f(x)$ on division by $(x-a_1)$. Since $a_1 \in C(R)$ we have

$$g(x)(x-a_1) = (x-a_1)g(x).$$

Hence $k(x) = g(x)$ and $f_L(a_1) = f_R(a_1) = f(a_1)$ above. Thus if $f(a_1) = 0$ we have

$$f(x) = g(x)(x-a_1) \qquad g(x) \in R[x]$$

where the degree of $g(x)$ is n-1. Now suppose $f(a_2) = 0$, and $a_2 \in C(R)$. Then

$$0 = f(a_2) = g(a_2)(a_2-a_1)$$

and $(a_2-a_1) \in C(R)$ since $C(R)$ is a ring. If $a_2 \neq a_1$, we must have $g(a_2) = 0$ in so far as $C(R)$ is without proper divisors of zero. Repeating the above argument on $g(x)$ which is of degree n-1 we have

$$f(x) = g(x)(x-a_1) = h(x)(x-a_2)(x-a_1) \qquad h(x) \in R[x]$$

where the degree of $h(x)$ is n-2. We may do this at most n times obtaining the following

$$f(x) = d(x-a_1)(x-a_2)\ldots(x-a_n) \qquad a_i \in C(R),\ d \in R.$$

If $b \in C(R)$ is such that $f(b) = 0$, then $b-a_i = 0$ for some i, $1 \leq i \leq n$ by Theorem 13.

If R does not have a unit element, by Theorem 15 we may imbed it in a prime ring T with a unit. By the above argument there are at most n elements $c \in C(T)$ such that $f(c) = 0$ where $f(x) \in T[x]$. Since $C(R) \subseteq C(T)$, the desired result follows immediately. Q.E.D.

Theorem 17. If R is a prime ring and $h(x)$ is a monic polynomial of degree n with integral coefficients, then there exist

at most n elements $c \in C(R)$ such that $h(c) = 0$.

Proof: Suppose R has a unit and let

$$h(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_o$$

where a_i, $0 \leq i \leq n-1$, are integers. Let $b \in C(R)$, $b \neq 0$. Then clearly $g(x) = h(x)b \in R[x]$. The preceding Theorem asserts the existence of at most n elements $c \in C(R)$ such that

$$g(c) = [h(c)]b = 0.$$

Since $h(c) \in C(R)$ and $b \neq 0$, we must have $h(c) = 0$.

As above, if R has no unit, imbed it in a prime ring T with a unit and repeat the argument. Q.E.D.

We now recall the following facts which were stated previously. A necessary and sufficient condition for a prime ring R to be isomorphic to a subdirect sum of prime rings S_i is that there exist in R prime ideals P_i such that $R/P_i \cong S_i$ and $\bigcap_i P_i = (0)$. Further, if $P_i \neq (0)$ for all $i \in I$, then R has a proper representation as a subdirect sum of the prime rings R/P_i.

For convenience we use the following notation in the sequel. Let $\mathfrak{M}$, $\mathfrak{M}_i$, $\mathfrak{M}'$, $\mathfrak{M}_i'$ designate a set of ideals, usually prime, in a prime ring R. Similarly, $\mathfrak{A} = \bigcap \mathfrak{M}$, $\mathfrak{A}' = \bigcap \mathfrak{M}'$, $\mathfrak{A}_i = \bigcap \mathfrak{M}_i$, and $\mathfrak{A}_i' = \bigcap \mathfrak{M}_i'$.

It is of interest to observe that a prime ring R can not have a proper representation as a subdirect sum of a finite number of rings. For suppose $R \cong \dotplus_{i=1}^{n} S_i$, $S_i \ncong R$ for $1 \leq i \leq n$. There exists, then, a finite number of ideals J_i $(i=1,2,\ldots,n)$ in R such that

$$R/J_i \cong S_i \qquad \text{and} \qquad \bigcap_{i=1}^{n} J_i = (0)$$

Since

$$J_1J_2\ldots J_n \subseteq J_1 \cap J_2 \cap \ldots \cap J_n = (0)$$

and R is prime $J_k = (0)$ for some k, $1 \leq k \leq n$. But then $R/J_k = R$, which is a contradiction.

The following result due to Krull [7] will be useful in proving the principal theorem of this chapter.

Theorem 18. Let I be an indexing set. If the prime ring R is isomorphic to a subdirect sum of prime rings S_i $(i \in I)$ and the set $\{N(S_i) \mid i \in I\}$ is bounded, then $N(R) < \infty$.

Proof: Recall that N(R) denotes the cardinality of C(R). By hypothesis there exists a positive integer M such that $q_i = N(S_i) < M$ for all $i \in I$. By Theorem 13 each $C(S_i)$ is zero or a finite field with less than M elements. Since any two finite fields with the same number of elements are isomorphic, there exist at most a finite number, say n, of non-isomorphic fields with fewer than M elements.

The nonzero elements of $C(S_i)$ form a multiplicative group of order $q_i - 1$. Hence for each $s_i \in C(S_i)$, $s_i^{q_i - 1} = 1$; i.e. each $s_i \in C(S_i)$ is a root of the polynomial

$$g_{q_i}(x) = x^{q_i} - x.$$

Hence, for each $s \in \bigcup_{i \in I} C(S_i)$, s is a root of the following monic polynomial with integral coefficients;

$$f(x) = (x^{q_1} - x)(x^{q_2} - x)\ldots(x^{q_n} - x).$$

Now we consider the homomorphism

$$h_i: R \longrightarrow S_i$$

induced by the subdirect sum representation. If $r \in C(R)$, then for each $x \in R$ and all $i \in I$,

$$h_i(r)h_i(x) = h_i(x)h_i(r)$$

and thus $h_i(r) \in C(S_i)$ for each $i \in I$.

We assert that $f(r) = 0$ for every $r \in C(R)$. Let the isomorphism between R and the subdirect sum of the S_i be given by

$$r \longleftrightarrow (s_1, s_2, \ldots).$$

Then

$$f(r) \longleftrightarrow f(s_1, s_2, \ldots) = (f(s_1), f(s_2), \ldots)$$

and under h_i, $f(r) \longrightarrow f(s_i)$. Suppose $r \in C(R)$ and $f(r) \neq 0$. Then for some i, $f(s_i) \neq 0$ and from above $s_i \notin \bigcup_{i \in I} (C(S_i))$. However, $h_i(r) = s_i \in C(S_i)$ for all $i \in I$. This is a contradiction. Thus $f(r) = 0$ for all $r \in C(R)$ and by Theorem 17 $C(R)$ is finite. Q.E.D.

The following two lemmas will be basic for our purposes.

Lemma 11. Let R be a countable prime ring with an infinite center and let $\{p_i \mid i = 1,2,\ldots\}$ be a countable set of non-zero prime ideals in R with $\bigcap_{i=1}^{\infty} p_i = (0)$. Then we can choose a sequence p_{i_k} $(k = 1,2,\ldots)$ such that $\bigcap_{k=1}^{\infty} p_{i_k} = (0)$ and one of the following is true;

(1) $$N(R/p_{i_k}) = \infty \qquad (k = 1,2,\ldots)$$

(2) $$N(R/p_{i_k}) < \infty \text{ and } N(R/p_{i_k}) < N(R/p_{i_{k+1}}) \qquad (k = 1,2,\ldots).$$

Proof: Let

$$\mathcal{M} = \{p_i \mid p_i \text{ is a prime ideal of } R,\ i = 1,2,\ldots\}$$

and

$$\mathcal{M}_1 = \{p_i \mid p_i \in \mathcal{M},\ N(R/p_i) = \infty\}$$

$$\mathcal{M}_2 = \{p_i \mid p_i \in \mathcal{M},\ N(R/p_i) < \infty\}.$$

If $\mathcal{A}_1 = \cap \mathcal{M}_1$ and $\mathcal{A}_2 = \cap \mathcal{M}_2$, then $\mathcal{A}_1 \cap \mathcal{A}_2 = (0)$ since $\mathcal{M} = \mathcal{M}_1 \cup \mathcal{M}_2$ and by hypothesis $\cap \mathcal{M} = (0)$ we have

$$(0) = \cap \mathcal{M} = (\cap \mathcal{M}_1) \cap (\cap \mathcal{M}_2) = \mathcal{A}_1 \cap \mathcal{A}_2.$$

If $\mathcal{A}_1 = (0)$, then (1) holds for a sequence in $\mathcal{M}$ consisting of those ideals in $\mathcal{M}_1$. We claim that if $\mathcal{A}_1 \neq (0)$, then $\mathcal{A}_2 = (0)$. For suppose $x \in \mathcal{A}_1$, $x \neq 0$ and let $y \in \mathcal{A}_2$. Then $(x) \subseteq \mathcal{A}_1$, $(y) \subseteq \mathcal{A}_2$ and further

$$(x)(y) \subseteq \mathcal{A}_1 \cap \mathcal{A}_2 = (0).$$

Since R is prime, $(x) = (0)$ or $(y) = (0)$. Since $(x) \neq (0)$, $y = 0$. Thus $\mathcal{A}_2 = (0)$.

Since R is countable, we can enumerate the nonzero elements of R in a sequence, say $a_1, a_2, \ldots$. Because $\mathcal{A}_2 = \cap \mathcal{M}_2 = (0)$ there exists $p_{i_1} \in \mathcal{M}_2$ such that $a_1 \notin p_{i_1}$. Let

$$\mathcal{M}_2' = \{p_i \mid p_i \in \mathcal{M}_2,\ N(R/p_i) \leq N(R/p_{i_1})\}$$

and

$$\mathcal{M}_2'' = \{p_i \mid p_i \in \mathcal{M}_2,\ N(R/p_i) > N(R/p_{i_1})\}.$$

Then $\mathcal{M}_2 = \mathcal{M}_2' \cup \mathcal{M}_2''$ and letting $\mathcal{A}_2' = \cap \mathcal{M}_2'$, $\mathcal{A}_2'' = \cap \mathcal{M}_2''$,

$$\mathcal{a}_2 = \cap \mathcal{m}_2 = (\cap \mathcal{m}_2') \cap (\cap \mathcal{m}_2'') = \mathcal{a}_2' \cap \mathcal{a}_2'' = (0).$$

We claim that $\mathcal{a}_2' \neq (0)$. For suppose $\mathcal{a}_2' = (0)$. By Theorem 2, R is isomorphic to a subdirect sum of the rings R/p_i, p_i an element of $\mathcal{m}_2'$. Further, for any $p_i \in \mathcal{m}_2'$, $p_i \neq (0)$; (if $p_j = (0)$ for some j, $N(R/p_j) = N(R)$ and N(R) would be finite). Thus this representation must be nontrivial and by Theorem 18, $N(R) < \infty$ which implies a contradiction. Hence $\mathcal{a}_2' \neq (0)$. As before, we must have $\mathcal{a}_2'' = (0)$ and there must exist $p_{i_2} \in \mathcal{m}_2''$ such that $a_2 \notin p_{i_2}$. Note that $N(R/p_{i_1}) < N(R/p_{i_2})$. Now let

$$\mathcal{m}_3' = \left\{ p_i \mid p_i \in \mathcal{m}_2'',\ N(R/p_i) \leq N(R/p_{i_2}) \right\}$$

and

$$\mathcal{m}_3'' = \left\{ p_i \mid p_i \in \mathcal{m}_2'',\ N(R/p_i) > N(R/p_{i_2}) \right\}.$$

We may repeat the above argument obtaining a sequence of prime ideals p_{i_k} $(k = 1,2,\ldots)$ such that $a_k \notin p_{i_k}$. Thus $\bigcap_k p_{i_k} = (0)$ and moreover $N(R/p_{i_k}) < N(R/p_{i_{k+1}})$ for $k = 1,2,\ldots$. Q.E.D.

Lemma 12. Let J be an ideal of R and $c \in R$, $\bar{c} \in C(R/J)$. If x is an indeterminate, then $R[x]/(J,x-c) \cong R/J$. In particular if J is a prime ideal in R, then (J,x-c) is a prime ideal in R[x].

Proof: We remark that we do not necessarily assume R to have

a unit. Also, $(J,x-c)$ is to be interpreted as follows

$$(J,x-c) = \left\{ j + f(x)(x-c) \mid j \in J,\ f(x) \in R[x] \right\};$$

i.e. $(J,x-c)$ does not have the usual meaning of the sum of the ideals J and $(x-c)$. If $r \in R$, let $\bar{r}$ denote the residue class to which r belongs modulo J.

Consider the mapping $h: R[x] \longrightarrow R/J$ defined as follows:

$$h(a_o x^n + a_1 x^{n-1} + \ldots + a_n) = \bar{a}_o \bar{c}^n + \bar{a}_1 \bar{c}^{n-1} + \ldots + \bar{a}_n.$$

It is easily verified that $\bar{h}$ is a homomorphism of $R[x]$ onto R/J. Now

$$\ker_h = \left\{ g(x) \in R[x] \mid h(g(x)) \in J \right\}$$

$$= \left\{ g(x) \in R[x] \mid \overline{g(c)} = 0 \right\}$$

$$= \left\{ g(x) \in R[x] \mid g(x) \equiv f(x)(x-c),\ f(x) \in R[x] \right\}$$

$$= \left\{ g(x) \in R[x] \mid g(x) \equiv f(x)(x-c) \bmod J,\ f(x) \in R[x] \right\}.$$

Hence we have that

$$\ker_h = \left\{ g(x) \in R[x] \mid g(x) = j + f(x)(x-c)\ j \in J,\ f(x) \in R[x] \right\}$$

$$= (J,x-c).$$

By the Fundamental Theorem of Homomorphisms we have

$$R[x]/(J,x-c) \cong R/J.$$

If J is prime, R/J is a prime ring. Hence $R[x]/(J,x-c)$ is a prime ring and $(J,x-c)$ is prime in $R[x]$. Q.E.D.

We are now in a position to prove the main theorem of the

chapter. McCoy's version generalizes a result first proved by Krull[7]. This theorem is a vivid illustration of the problem stated at the beginning of the chapter. We are given a countable set of prime rings R_i and we look at the various subdirect sums of these rings and ask the following question;

Under what conditions does R[x], where R is a given ring of a specific type, have a representation as a subdirect sum of the prime rings R_i? The answer is to be found in the following important result.

Theorem 19. Let R be a countable prime ring with infinite center. If R has a non trivial representation as a subdirect sum of a countable number of prime rings R_i (i = 1,2,...), then R[x] also has a non trivial representation as a subdirect sum of the prime rings R_i.

Proof: By hypothesis there exists a countable number of non-zero prime ideals p_i of R (i = 1,2,...) such that $\bigcap_{i=1}^{\infty} p_i = 0$ and $R/p_i \cong R_i$. In Lemma 12 let $J = p_i$ and $c = 0$. Then $R/p_i \cong R_i$ is a homomorphic image of R[x] for each i. If we can show that R[x] is isomorphic to a subdirect sum of some of the rings R_i, then by Theorem 1, R[x] will be isomorphic to a subdirect sum of the rings R_i.

By Lemma 11 there exists a sequence $p_{i_k} \subseteq p_i$ (k = 1,2,...) such that $\bigcap_{k=1}^{\infty} p_{i_k} = (0)$ and one of the following holds

(1) $N(R/p_{i_k}) = \infty$ (k = 1,2,...)

or

$$(2)\quad \left\{ \begin{array}{ll} & N(R/p_{i_k}) < \infty \\ \text{and} & \\ & N(R/p_{i_k}) < N(R/p_{i_{k+1}}) \qquad (k = 1,2,\ldots). \end{array} \right.$$

We claim that for any positive integer s

$$(3)\quad \bigcap_{k=s}^{\infty} p_{i_k} = (0)$$

The proof of this is by induction on k. Clearly it is true for k = 1. Assume $\bigcap_{k=n}^{\infty} p_{i_k} = (0)$ for some $n \geq 2$. Let $J = \bigcap_{k=n+1}^{\infty} p_{i_k}$.

Then J is an ideal in R and

$$\bigcap_{k=n}^{\infty} p_{i_k} = p_{i_n} \cap J = (0).$$

However, $p_{i_n} J \subseteq p_{i_n} \cap J = (0)$. Since R is a prime ring $p_{i_n} = (0)$ or $J = (0)$. But $p_{i_n} \neq (0)$, hence $\bigcap_{k=n+1}^{\infty} p_{i_k} = (0)$.

For any positive integer r, the number of ideals p_{i_k} such that $N(R/p_{i_k}) \leq r$ is finite. Hence for any positive integers r and s the set

$$\left\{ p_{i_k} \mid k \geq s,\ N(R/p_{i_k}) \leq r \right\}$$

is finite. Therefore, the set

$$F(s,r) = \left\{ p_{i_k} \mid k \geq s,\ N(R/p_{i_k}) > r \right\}$$

is infinite and from above (3) we have

(4) $$\bigcap_{k=s}^{\infty} F(s,r) = (0).$$

Let $f_1(x)$, $f_2(x)$,.... be nonzero elements of R[x] of arbitrary order. By equation (4) with s = 1 and r = deg $f_1(x)$

$$\bigcap_{k=1}^{\infty} \left\{ p_{i_k} \mid k \geq 1,\ N(R/p_{i_k}) > \deg f_1(x) \right\} = (0).$$

Let

$$A = \left\{ p_{i_k} \mid k \geq 1,\ N(R/p_{i_k}) > \deg f_1(x) \right\}.$$

If all the ideals of A contained all coefficients of $f_1(x)$, then $\bigcap_{k=1}^{\infty} A \neq (0)$. Hence there exists at least one ideal of A which does not contain all coefficients of $f_1(x)$. Let $p_{i_{k_1}}$ be the first such prime ideal. (Recall that all ideals in A are prime.) Now $R/p_{i_{k_1}}$ is prime and we consider $\bar{f}_1(\bar{x}) \in (R/p_{i_{k_1}})[x]$. Since $p_{i_{k_1}}$ does not contain all coefficients of $f_1(x)$,

$$\deg \bar{f}_1(\bar{x}) < \deg f_1(x).$$

If deg $f_1(x) = k$, then Theorem 16 asserts the existence of at most k elements $\bar{c} \in C(R/p_{i_{k_1}})$ such that $\bar{f}_1(\bar{c}) = 0$. However, since $p_{i_{k_1}} \in A$, $N(R/p_{i_{k_1}}) > k$ and hence there exists at least one element $\bar{c} \in C(R/p_{i_{k_1}})$ such that $\bar{f}_1(\bar{c}) \neq 0$. Let

$$(p_{i_{k_1}}, x-c) = p_{i_{k_1}}[x].$$

Then by Lemma 12, $p_{i_{k_1}}[x]$ is prime in $R[x]$ and by the proof of that lemma $f_1(x) \notin p_{i_{k_1}}[x]$. Also we have that

$$R[x]/p_{i_{k_1}}[x] \cong R/p_{i_{k_1}} \cong R_{i_{k_1}}.$$

To complete the proof we use an inductive process. Suppose prime ideals $p_{i_{k_j}}[x] \subsetneq R[x]$ $(j = 1,2,\ldots,n)$ have been found such that

$$f_j(x) \notin p_{i_{k_j}}[x] \qquad (j = 1,2,\ldots,n)$$

and

$$R[x]/p_{i_{k_j}}[x] \cong R_{i_{k_j}} \qquad (j = 1,2,\ldots,n).$$

We may also assume $i_{k_1} < i_{k_2} < \cdots < i_{k_n}$. By equation (4)

$$\bigcap_k \left\{p_{i_k} \mid k > i_{k_n},\ N(R/p_{i_k}) > \deg f_{n+1}(x)\right\} = (0).$$

Let $p_{i_{k_{n+1}}} \in \left\{p_{i_k} \mid k > i_{k_n},\ N(R/p_{i_k}) > \deg f_{n+1}(x)\right\}$ be the first one not containing all the coefficients of $f_{n+1}(x)$.

As above, there exists $\bar{d} \in C(R/p_{i_{k_{n+1}}})$ such that

$$\bar{f}_{n+1}(\bar{d}) \neq 0.$$

This implies that

$$f_{n+1}(x) \notin (p_{i_{k_{n+1}}}, x-d) = p_{i_{k_{n+1}}}[x].$$

It is clear that this process can be continued obtaining a

sequence

$$p_{i_{k_1}}[x],\ p_{i_{k_2}}[x],\ldots$$

of nonzero prime ideals in R[x] such that

$$\bigcap_{j=1}^{\infty} \left\{p_{i_{k_j}}[x]\right\} = (0)$$

since if $0 \neq f_u(x) \in \bigcap_{j=1}^{\infty} \left\{p_{i_{k_j}}[x]\right\}$, then $f_u(x) \in p_{i_{k_u}}[x]$, which is a contradiction. Hence by Theorem 2 R[x] is isomorphic to a subdirect sum of the rings $R[x]/p_{i_{k_j}}[x]$ and by Lemma 12

$$R[x]/p_{i_{k_j}}[x] \cong R/p_{i_{k_j}} \cong R_{i_{k_j}} \qquad (j = 1,2,\ldots).$$

We now explicitly show that R[x] is isomorphic to a subdirect sum of the R_i (i = 1,2,...) knowing that it is isomorphic to a subdirect sum of the rings $R_{i_{k_j}}$ (j = 1,2,...). For each $0 \neq r(x) \in R[x]$ there exists $0 \neq r_{i_{k_u}} \in R_{i_{k_u}}$; i.e. if

$$h_{i_{k_u}} : R[x] \longrightarrow R_{i_{k_u}}$$

is the homomorphism $h_{i_{k_u}}(r(x)) = r_{i_{k_u}} \neq 0$. Thus for each non-zero $r(x) \in R[x]$, $h_{i_{k_j}}(r(x)) \neq 0$ for at least one j. By Theorem 1 R[x] is isomorphic to a subdirect sum of the rings R_i.

Since $p_i \neq (0)$ (i = 1,2,...), $p_i[x] = (p_i, x-c) \neq 0$

$(i = 1,2,\ldots)$ for $\overline{c} \in C(R/p_i)$. Thus the representation of $R[x]$ is in fact proper and the proof is completed.

BIBLIOGRAPHY

1. Birkhoff, G., "Subdirect unions in universal algebra," Bulletin of the American Mathematical Society, vol. 50, 1944, pp. 764-768.

2. Birkhoff, G. and MacLane, S., A Survey of Modern Algebra, Macmillan Company, New York, 1953.

3. Forsythe, A. and McCoy, N.H., "On the commutativity of certain rings," Bulletin of the American Mathematical Society, vol. 52, 1946, pp. 523-526.

4. Köthe, G., "Abstrakte Theorie nichkommutativer Ringe mit einer Anwendung auf die Darstellungstheorie kontinuierlicher Gruppen," Mathematische Annalen, vol. 103, 1930, pp. 545-572.

5. Köthe, G., "Ein Beitrag zur Theorie der kommutativen Ringe ohne Endlichkeitsbedingung," Nachrichten Gesellschaft der Wissenschaften zu Göttingen, 1930, pp. 195-207.

6. Krull, W., "Idealtheorie in Ringen ohne Endlichkeitsbedingung," Mathematische Annalen, vol. 101, 1929, pp. 729-744.

7. Krull, W., "Subdirekte Summendarstellungen von Integritätsbereichen," Mathematische Zeitschrift, vol. 52, 1950, pp. 810-826.

8. McCoy, N.H. and Montgomery, D., "A representation of generalized Boolean rings," Duke Mathematical Journal,

vol. 3, 1937, pp. 455-459.

9. McCoy, N.H., "Subdirect sums of rings," Bulletin of the American Mathematical Society, vol. 53, 1947, pp. 856-877.

10. McCoy, N.H., "Subdirectly irreducible commutative rings," Duke Mathematical Journal, vol. 12, 1945, pp. 381-387.

11. McCoy, N.H., "Subdirect sum representations of prime rings," Duke Mathematical Journal, vol. 22, 1955, pp. 357-363.

12. McCoy, N.H., Rings and Ideals, Carus Monographs, Mathematical Association of America, 1948.

13. Prüfer, H., "Neue Begründung der algebraischen Zahlentheorie," Mathematische Annalen, vol. 94, 1925, pp. 198-243.

14. Stone, M.H., "The theory of representations for Boolean algebras," Transactions of the American Mathematical Society, vol. 40, 1936, pp. 37-111.

15. von Neumann, J., "On regular rings," Proceedings of the National Academy of Sciences of U.S.A., vol. 22, 1936, pp. 707-713.

VITA

On October 15, 1940 Robert J. McNelis was born the son of Francis A. and the late Mary E. McNelis. After an elementary and secondary education in the Wilkes-Barre City school system, he was graduated in 1958 from G.A.R. Memorial high school. In 1962 he received, with honors, the degree of Bachelor of Arts with a major in mathematics from King's College. Presently he is studying under a National Defense Education Act Fellowship at Lehigh University.

He is engaged to marry Maria Elena Mohen in August of this year.